Building a Deterrence Policy Against Strategic Information Warfare

Geoffrey S. French, Veridian
10455 White Granite Drive, Suite 400
Oakton, Virginia 22124
geoff.french@veridian.com

Abstract

As the United States continues as the sole nation with a vested interest in every region of the world, it is increasingly sensitive to asymmetric threats that neutralize or circumvent its ability to defend against or respond to hostile activity. One of these areas is broadly described as *information warfare*. One specific aspect of this refers to strategic information warfare (SIW) attack against the information technology base of the nation's critical infrastructures. Defending those infrastructures is problematic for the U.S. government. Although the military relies on the civilian infrastructure, it does not control it. Neither is the civilian government in a position to dictate to the private infrastructure organizations. Any attempts to defend the national information infrastructure may be based largely, therefore, on deterring an attack, rather than detecting and thwarting it. Although deterrence may be most commonly associated with nuclear warfare, the United States still relies to a large extent on deterring aggressive foreign activity to protect its interests worldwide. This paper assesses the threat from SIW attacks and reviews the theories of deterrence, focusing on deterrence in the post-Cold War era. It then describes some strategies the United States can build to deter SIW most effectively.

Introduction

At the beginning of the 21st century, the United States finds itself the sole nation with a vested interest in the political and military events in every region of the world. This comes at a time when the economies of individual nations have become intertwined around the globe at an unprecedented level. The advantage of this interdependence is that it tends to support stability in most regions of the world. The disadvantage is that almost any regional conflict can be interpreted as a threat to U.S. interests, based largely on its proximity to U.S. allies or key natural resources. All of these factors contribute to a general need for the United States to maintain a global military presence. One of the effects

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **JUN 2002**	2. REPORT TYPE	3. DATES COVERED **00-00-2002 to 00-00-2002**

4. TITLE AND SUBTITLE **Building a Deterrence Policy Against Strategic Information Warfare**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Veridian,10455 White Granite Drive Suite 400,Oakton,VA,22124**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

2002 Command and Control Research and Technology Symposium

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**13**	

of this global presence is the hope that force will not be needed, that is, that U.S. interests will not be attacked simply because the United States has the means to retaliate. This hope is largely a continuation of the policy of deterrence, developed formally during the Cold War.

As is evident from current events, however, not every action is deterred, and the United States continues to have a number of adversaries in different parts of the world. As it engages in many low-level military actions, from ground assaults to air support to peacekeeping, the United States is increasingly sensitive to asymmetric threats to its power. That is to say that even as the United States wields tremendous conventional military strength and maintains a nuclear arsenal, it is concerned about methods of attack that neutralize or circumvent its ability to defend against or respond to hostile activity. One of these areas is broadly described as *information warfare* (IW). IW poses a unique threat to the United States in that it is not only a potential threat to U.S. security, but also because it presents specific problems to U.S. deterrence. The following sections examine this problem, explain the concept of strategic IW, examine deterrence theory, and present conclusions about how deterrence policies may be created to face this specific and emerging threat.

21st Century Deterrence and the Problem of Information Warfare

U.S. deterrence has changed dramatically over the past ten years. Although the concept of deterrence can be found as far back as ancient texts that discuss military strategy, the word itself does not appear until the nuclear era.[1] Deterrence theory, therefore, has largely gone hand-in-hand with nuclear policy. President George Bush's reduction of the alert status of the strategic bombers in 1991, however, marked the end of the primary focus of U.S. deterrence: preventing an attack by the Soviet Union. Since that time, the U.S. deterrent has shifted from a reliance on nuclear forces to a reliance on conventional forces. Although conventional forces clearly played a role in deterrence prior to 1991 and nuclear forces continue to play a deterrent role, several changes have made U.S. conventional forces capable of providing a significant deterrent effect. First, their technological sophistication makes them a much more effective lethal force than any U.S. adversary's. Second, their logistical support allows them to deploy in any part of the world rapidly. Finally, the U.S. government has been willing to use them in a large number of low-level conflicts and a few important high-level conflicts.[2] Taken together, this means that adversaries can expect the United States to use its military in situations where its interests are threatened and with a very high expectation of success.

[1] J. D. Steinbrunner, "Revising the practice of deterrence," In: *Post-Cold War Conflict Deterrence*, National Research Council, Naval Studies Board, (Washington D.C.: National Academy Press, 1997).

[2] G. L. Guertner, "Deterrence and conventional military forces," In: *Deterrence in the 21st Century*, M. G. Manwaring (ed.), (Portland, Ore.: Frank Cass, 1999).

Countering U.S. Military Dominance

Adversaries' reactions to the use of U.S. force, however, cause them to look for methods to counter this superiority. Just as the United States used its nuclear forces to counter a superior conventional Soviet military threat in Europe after World War II, other nations will attempt to obtain weapons that negate or circumvent U.S. strength. Hence, the constant pursuit of nuclear weapons by such nations as Iraq, Iran, and North Korea. Another possible way of doing this is through the development of IW programs. Although a broad definition of IW includes any "actions taken to affect adversary information or information systems,"[3] in a strategic military context the definition must focus on the targeting and attacking of an adversary's information infrastructure (i.e., the "information resources, including communications systems, that support an industry, institution, or population"[4]) in an attempt to cause the defeat of that adversary's military or government. (This is discussed in further detail below.)[5]

Two potential targets for a strategic IW strike are (1) the information base of the U.S. military and (2) U.S. civilian information infrastructure. There are three major advantages to attacking civilian targets as opposed to military targets. First, they are softer targets. Adversaries can expect that to some extent the United States has taken steps to protect its military infrastructure by hardening physical cyber components and adopting defensive measures. The civilian infrastructure, in contrast, is controlled by the myriad public and private organizations that constitute the infrastructure and have much less uniformity in security awareness (much less policy and implementation). Second, civilian targets offer the possibility of cyber attacks with nation-wide effects. An adversary in conflict with the United States can have little expectation to affect the area outside of its immediate control, except through unconventional attacks. Ballistic missiles are one method of extending a military's range, but even these can be infeasible against the United States. For most nations, ballistic missiles (regardless of the payload) are an expensive investment and could be preempted in a crisis situation. Cyber attacks, however, would be difficult (if not impossible) to detect and preempt, and could offer an adversary the ability to affect large parts of the United States. Third, the U.S. military relies in many ways on the civilian infrastructure,[6] and a strategic attack on that infrastructure could affect the military to a greater extent than a direct conventional attack. Cyber attacks would have the advantage of affecting both the U.S. military and the civilian population.

[3] The U.S. Department of Defense defines *information warfare* as "information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries." *Information operations* are defined as "actions taken to affect adversary information and information systems while defending one's own information and information systems." See Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms.*

[4] D. Denning, *Information Warfare and Security* (Reading, Mass: Addison-Wesley, 1999).

[5] For a more in-depth discussion of the scope of information warfare, see Martin C. Libicki's paper "What is Information Warfare?" (Washington D.C.: National Defense University, 1995).

[6] F. Cillufo, J.J. Collins, A. de Borchgrave, D. Goure, and M. Horowitz, *Defending America in the 21st Century*, (Washington D.C.: Center for Strategic and International Studies, 2000).

The Conundrum of SIW

Defending the civilian infrastructure is problematic for the U.S. government. Although the military relies on the civilian infrastructure (such as satellite communications networks), it does not control it. Neither is the civilian government in a position to dictate to the private owners of the infrastructure. Despite the many government entities with missions to protect the nation's infrastructure, the U.S. government is still in the process of forging partnerships with infrastructure-related industries and entities. The government's role (and especially that of the U.S. military) in defending the national information infrastructure may be based largely, therefore, on deterring a cyber attack, rather than detecting and thwarting an attack. The United States is then faced with the conundrum of deterring an ability that an adversary developed to counter U.S. strength. This very specific type of deterrence, therefore, must be carefully tailored to the threat. This requires a better understanding of the circumstances in which the United States may face a strategic cyber attack and the methods the United States has at its disposal to deter any type of attack.

Understanding Strategic IW Attack

Although volumes have been produced on the topic, IW is one of the more confusing modern concepts because so many organizations or authors use the term to mean a host of definitions. The two tendencies that have caused the most expansion of the term are (1) the inclusion of any illegal computer-related activity or unintended use of information technology, and (2) the inclusion of any activity intended to affect the decision-making process on any level. Of the many activities that have been categorized as IW, therefore, include:

- web page defacements;
- any self-replicating malicious code;
- on-line fraud and bank robbery;
- computer-based espionage;
- psychological operations; and
- strategic deception, propaganda, and lying.

Upon reflection, however, it is clear that many of these activities are simply not acts of war. Although many authors will agree with the argument that information warfare is about "'warfare' in the most general sense, encompassing certain types of crime as well as military operations,"[7] when discussing defense policy, the first contraction of the term must be to limit the discussion to military matters. Even this is not sufficient, however. A review of military-specific IW literature reveals two other expansions of the term to include (1) any type of technologically sophisticated warfare, such as stealth aircraft and smart bombs, and (2) any type of information-intensive maneuver, embodied in the concept of network-centric warfare.[8]

[7] D. Denning, *Information Warfare and Security* (Reading, Mass: Addison-Wesley, 1999).

[8] G. French, "Shunning the frumious Bandersnatch: Current literature on information warfare and deterrence," Information Warfare Research Center, 2000.

A more focused definition would limit the activities to those that attempt to affect the information technology base of a military or nation and that are intended to lead to a military gain. Some have further focused on the aspect of IW to examine the potential for attacking a nation's information infrastructure.[9] A working definition for a strategic infrastructure attack is a series of computer-based attacks against the information technology–base of the critical national infrastructures. These infrastructures include:

- Banking and Finance,
- Electric Power,
- Emergency Response,
- Government Operations,
- Oil and Gas,
- Telecommunications,
- Transportation, and
- Water Supply and Wastewater Treatment.

In this context, an acceptable definition of strategic IW is "coordinated, systematic attacks against the United States through computers, communications systems, databases, and media."[10] Throughout this paper, SIW will refer to a nation-wide cyber attack on the U.S. information infrastructure designed to achieve the strategic goal of defeating the U.S. military or a long-term instability in the United States. IW will be used to reflect the more general ability to attack the information technology base of a military or nation. Having defined the issue, it is possible to discuss countries likely to launch such an attack and the circumstances where one would most likely to be encountered.

Identifying IW Capabilities

There are a number of reasons why the nations with established and potent IW programs are largely unknown. Primarily, the indicators of such a program differ from any other. Conventional military strength, for example, is easily detected and assessed. Nations must either purchase weapons systems or have the industrial capacity to build them. Moreover, the more powerful the weapon system (e.g., tanks, aircraft, and naval vessels), the easier it is to detect. IW programs, however, also differ from other non-conventional weapons programs. IW programs do not require the detectable engineering research, development, testing, and evaluation that complex weapon platforms such as ballistic missiles require. They do not require the concentration of highly specialized knowledge (or the program signatures) that nuclear, biological, or chemical weapons programs do. Funding an IW program can be done clandestinely, and with direction, it can be masked as legitimate businesses or research and development.

[9] To be complete, Michael Wilson has written multiple papers on "Infrastructural Warfare" (IWAR). Identifying his precise definition can be challenging. The 1997 paper "Waging IWAR" offers the closest approximation of a definition, as follows. "IWAR in fact represents a meta-model that enables movement from conflict context to context while preserving and expanding a warrior's ability to engage an opponent. IWAR is nothing new, nor is it particularly a revelation; it is an abstraction drawn from the process of history: conflict oriented to or from the infrastructure of a society."

[10] Center for Strategic and International Studies, *Cybercrime, Cyberterrorism, Cyberwarfare* (Washington D.C.: Center for Strategic and International Studies, 1998).

For these reasons, the list of nations with capable IW programs are somewhat speculative, especially as they include nations other than those with historically strong intelligence programs. Even so, estimates can be made. In 2000, the U.S. Navy described the following nations as potential threats for conducting information operations (IO).

> Virtually any state, group—even friendly or neutral—can use IO to attack other nations. Four countries—Russia, China, India, and Cuba—currently have an acknowledged IO policy and a rapidly developing IO capability. Rogue states, such as North Korea, Iran, Iraq, Libya, and Syria have some IO capability and may covertly employ it at any time that suits their needs. Many other nations, including France, Japan, and Germany, are players in IO and are also potential proliferators of IO capabilities to other states.[11]

This general breakdown is also useful for categorizing the threats into different level, separating allies from regional powers and rogue nations. A further delineation can also be made between major (Russia and the People's Republic of China) and minor (India and Cuba) military powers that may instigate or become entangled in a regional conflict that could involve the United States. Major powers have established, proven, and well-funded intelligence capabilities, high technology expertise, and a high degree of connectivity in terms of telecommunications and computers. A rough estimate would therefore place them at the high end of the threat spectrum. Minor powers may have intelligence services as aggressive as those of major powers, technical expertise, or good connectivity, but not likely all three, and therefore are likely to be less likely to be a high threat for SIW. Rogue states are especially unlikely to have all three advantages to a create a potent SIW threat given that they tend to be hampered by poor telecommunication infrastructures, which would be needed to support an indigenous IW program capable of SIW. In addition, rogue nations usually have closed societies. They tend to rely, therefore, on expatriate citizens to provide a window into certain technologies and information technology is one type. This puts them at a further disadvantage and, therefore, the low end of the threat spectrum.

To this catalogue of threats, one final category should be added: terrorist groups. Terrorists groups are harder to predict in that they have well-funded activity in specific areas, and could therefore develop in-depth technical expertise. They may also have intelligence or other assistance from nation states that could compensate for other disadvantages. Although they are not likely to present a highly sophisticated threat, they may pose a more heightened threat than rogue states. Although one could argue for other groups to be included, such as hackers or organized crime syndicates, they are not likely to meet the scope of strategic IW attacks. Furthermore, their activity is most likely to be treated as a criminal matter and pursued by law enforcement or counterintelligence, not the defense community.

[11] U.S. Navy, Chief of Naval Operations, *Navy Strategic Planning Guidance* (available at http://www.hq.navy.mil/n3n5/files/NSPG2000.pdf) 2000.

Estimating the Probability

A number of assessments of probability for use of IW have been done. Many of these have tended to focus, however, on the anonymous, surprise attack.[12] These ignore the fact that most attacks take place with a political context. Even Pearl Harbor occurred in a political-military context, and even Al-Qaida claimed responsibility for the terrorist attacks on September 11, 2001. More realistic assessments focus on IW attacks against military targets, but even these are useful. Kenneth McKenzie, Jr., for example, identifies IO as being most likely to be utilized in crisis situation, that is, prior to deployment of U.S. troops.[13] McKenzie also explores the possibility of an SIW strike against civilian infrastructure, but without comment to its likelihood. Even so, his approach is sound in that different types of adversaries have differing inclinations of engaging in SIW. The following sections (summarized in Table 1) look at SIW within context of the categories described above.

Major Regional Powers

Although major regional powers are not likely to provoke a direct confrontation with the United States, they may instigate a regional conflict that could threaten U.S. interests and therefore involve the United States. In a situation in which a major power anticipates U.S. involvement, it may use IW to delay U.S. deployment, thereby giving itself the opportunity to present the world with a fait accompli. An SIW attack could have the same effect, and therefore may have some appeal. Such an attack, however, would likely have one of two effects. It would cause only a temporary effect but greatly escalate the U.S. response far greater than would be warranted for a regional conflict, or it would have a crippling effect and cause long-term damage to the U.S. economy and logistical support. This latter possibility would also lead to several consequences that would be unacceptable to any major power, given the nature of interdependent economies and the enormous amount of aid the United States provides.

Minor Regional Powers

Minor military powers, such as the former Republic of Yugoslavia, may also find themselves in conflict with the United States because of a regional conflict that grew to affect U.S. interests. In the case where a minor military power has some SIW capability, they will likely face the same calculation that major powers would, but may have less at stake from the loss of aid or trade if the United States suffers a crippling blow to its critical infrastructure. But unlike a major power, a minor state would have much more to fear from a U.S. conventional strike, in that its very existence could be threatened. In such a case, a minor power might use SIW as a desperate attempt at survival.

[12] See, for example, Steven Blank's "Can Information Warfare be deterred?" in *Information Age Anthology Volume III,* (Washington D.C.: DoD C4ISR Cooperative Research Program, 2001), and the discussion of deterrence in *Cybercrime, Cyberterrorism, Cyberwarfare* (Center for Strategic and International Studies, 1998).

[13] Kenneth McKenzie, Jr., *The Revenge of the Melians: Asymmetric Threats and the Next QDR* (Washington D.C.: National Defense University, 2000).

Rogue States

In contrast to regional powers, rogues states may come into, or even instigate, direct conflict with the United States. It is plausible that the United States could confront Iraq or Syria, for example, in its counterterrorism campaign. A rogue state would likely have even less concern for long-term damage to the United States than a minor regional power would, and would be more likely to see the conflict as a fight for its existence. If facing major hostile activity (such as an invasion), rogue states could be more likely to escalate to SIW attacks prior to U.S. deployment and as any military action progresses.

Terrorist Groups

Terrorist groups have not yet displayed proven capability in computer network attack. There are a number of reasons why terrorists have not pursued this more aggressively, including a historical preference for physical attacks over more sophisticated but less visible attacks, and the tendency to rely on members' expertise rather than to hire outside professionals.[14] Even so, some terrorist groups may have understood the significance of the effects of the September 11 attacks on the nation's infrastructure and look to repeat and broaden those effects in future attacks. Given their proven capability to conduct attacks coordinated over a wide geographic area, even a modest increase in sophistication of targeting could allow future attackers to attack cyber components whose disruption or destruction would have a nation-wide effect. In the foreseeable future, at least, terrorist attacks are likely to be focused on a specific geographic area rather than the entire United States. The probability of a terrorist SIW attack, therefore, is low.

Table 1: Estimated Threat of SIW Attack

Adversary	Estimated relative capability	Circumstances most likely to employ SIW	Estimated relative probability
Major power	High	Prior to U.S. deployment	Low
Minor power	Medium	Prior to U.S. deployment Prior to destruction of the state apparatus	Medium
Rogue state	Low	Prior to U.S. deployment Prior to destruction of the state apparatus	High
Terrorist group	Low to Medium	Peace	Low

[14] A. Rathmell, R. Overill, L. Valeri, and J. Gearson, "The IW threat from sub-state groups: An interdisciplinary approach," In: *Information Age Anthology Volume III*, D. Alberts and D. Papp (eds), (Washington D.C.: DoD C4ISR Cooperative Research Program, 2001).

Exploring Deterrence

Just as IW has a number of definitions and connotation that must be clarified, deterrence has a number of variation that should be explored for a thorough discussion. Deterrence, thankfully, is easier to define. The U.S. Department of Defense defines deterrence as "the prevention from action by fear of the consequences. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction."[15] From this simple notion, however, there are a number of interpretations or adaptations. The following sections explore the applications, forms, components, and tools of deterrence.

General and Specific Applications of Deterrence

Most discussions about deterrence reflect the DoD definition and describe general deterrence, where the United States (or applicable home of the discussant) seeks to prevent inimical actions. These, too, are defined broadly and usually involve any hostile action that disrupts strategic or regional stability and peace. It is in this light that Gary Wheatley and Richard Hayes argue that SIW attacks[16] are deterred "by the same policy that deters other types of attack," and that the United States "already has basic policies in place that serve as effective deterrents in many circumstances."[17] In his paper on "Information Operations, Deterrence, and the Use of Force," however, Roger Barnett argues that conclusions like this ignore an important aspect of deterrence: specific deterrence. In his words,

> "Focused," or " immediate," deterrence operates at a different level of specificity. It recognizes that sometimes general deterrence does not work—posturing without reference to a particular objective will be viewed as weak or irrelevant—and that a focused, immediate, or specific deterrent *threat* or *statement* is required. Thus, focused deterrence is "stronger" than general deterrence, representing a nation's explicit effort to dissuade an adversary from carrying out an undesirable act (or failing to carry out a desirable one).[18]

As can be seen from the conundrum described above and from the differing probabilities of encountering SIW strikes from different types of adversaries, SIW will require well constructed specific deterrent policies if it can be deterred at all.

[15] Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, (Washington D.C.: U.S. Department of Defense, 2001).

[16] Although Wheatley and Hayes use the term *cyber war*, they define it to mean "attacks directed through computers and their connectivity." The highest level of this type of attack is a "strategic (catastrophic) attack" that includes targeting key industries, meeting the definition of strategic information warfare described above.

[17] G. F. Wheatley and R. E. Hayes, *Information Warfare and Deterrence* (Washington D.C.: National Defense University Press, 1996).

[18] R. Barnett, "Information operations, deterrence, and the use of force," *Naval War College Review* 51(2):7–19.

Forms of Deterrence

Barnett also defined two forms of deterrence: that from denial and that from punishment. Denial "requires stout defenses and a history of consistent refusals to yield to coercive threats." In regards to denying SIW attacks, however, he concludes "the ability of the United States and other open societies to deter an information attack by a strategy of denial is, and always will be, suspect."[19] In addition to these two forms, Paul Davis adds moral or social norms and lack of incentives.[20] Unfortunately, the former does not apply. First, IW does not carry the stigma that chemical, biological, or nuclear weapons do. Secondly, the United States has routinely attacked infrastructure targets. From the electric power grid of Belgrade to the pharmaceutical factory in Sudan, the United States has used conventional weapons against civilian infrastructure targets in its most recent actions. It is difficult, therefore, for the United States to argue that civilian infrastructure is an illegitimate target. Similarly, the incentives are also hard to deny. Although each type of adversary has different motivations, three of the four may have high incentives to launch SIW attacks in specific circumstances (see section "Estimating the Probability," above). For SIW attacks, therefore, deterrence will likely rely heavily on punishment, although the United States should clearly pursue the other three forms.

Components of Deterrence

There is more to creating a successful specific deterrent than to focus on a specific goal. Richard Harknett adds that there must be both the commitment to the goal and the ability to punish.[21] In the case of SIW, the United States plainly has both. Wheatley and Hayes would add that the threat to punish must be clear and communicated. The U.S. threat, although clear, is still in the rudimentary stage of being communicated. The Naval Studies Board of the National Research Council describes three other components of deterrence that complicate IW-related deterrence.[22] First, a successful deterrent requires quality intelligence. This is partially for communication purposes, and this is where the U.S. record is inconsistent at best, especially with regard to rogue states. The United States has seemed ill prepared to understand and persuade Iraq and North Korea to meet specific demands or suspend specific actions. Second, deterrence relies on the threats (or incentives) to be credible. Although the United States has the ability to retaliate, it is not known to what extent an SIW attack would disable certain military options. This erodes the certainty of punishment and therefore leaves some gap in any deterrent policy. Finally, the Naval Studies Board included applicability of the situation as a component to successful deterrence, noting that some adversaries—including terrorists—are "willing to pay any price" to achieve their goals. For SIW attacks, the United States has clear goals

[19] R. Barnett, "Information operations, deterrence, and the use of force," *Naval War College Review* 51(2):7–19.

[20] P. K. Davis, "Special challenges in extending deterrence in the new era," In: *Post-Cold War Conflict Deterrence,* National Research Council, (Washington D.C.: National Academy Press, 1997).

[21] R. J. Harknett, "Information warfare and deterrence." *Parameters* 1996 (Autumn):93–107.

[22] National Research Council, Naval Studies Board, *Post-Cold War Conflict Deterrence*, (Washington D.C.: National Academy Press, 1997).

and commitment, a very real threat (which may have a hint of doubt), but it must learn how to communicate that threat.

Tools of Deterrence

Finally, it is important to note that the United States has many tools to implement deterrence. Just as the U.S. Department of State communicates U.S. policy abroad and can emphasize the military threat if appropriate, the United States has other mechanisms of influencing foreign actions. International law can be one method of attempting to create the social norms that Paul Davis describes. The United States can attempt to encourage specific nations to renounce or relinquish specific types of weapons through bilateral or multilateral treaties or agreements. Timothy Thomas, among others, has argued that this may be a useful tool for IW as it has for nuclear weapons.[23] Both of these forms of influence, however, have had success only to the degree they are verifiable and enforceable. As argued above, SIW capability is very difficult to detect or prove. Moreover, without a very strong stigma, adversaries of the United States would likely not limit their SIW capabilities in a conflict, especially rogue nations, who tend to ignore international norms, and terrorists groups, who are not bound at all. A less formal option would be for the United States to participate in high-level discussions about the interconnected nature of the global economy. Some analysts, including Matthew Devost, have argued that this may be the most powerful deterrent, as "interdependence will act as a disincentive to state-sponsored information warfare."[24]

Tailoring Deterrence to SIW

Clearly, general deterrence remains a fundamental plank of U.S. security policy. Specific policies are required, however, to deter the more likely and more dangerous threats to U.S. interests. Deterring SIW in particular is a significant challenge. In many ways, SIW seems designed to erode confidence in the multiple forms of deterrence. It is meant to counter U.S. conventional strength (which generates the deterrent threat of punishment), it is difficult to defend (making denial undependable), and it contravenes no treaty or moral barrier (no more so than war), all of which make it a very attractive option for potential adversaries (increasing the incentives to pursue such a program). A deliberately formed deterrent policy, therefore, must match certain achievable aspects of each form of deterrence to specific adversaries. The following sections (summarized in Table 2) describe the tools and forms of deterrence most likely to be successful against potential adversaries.

[23] T. L. Thomas, "Deterring information warfare: A new strategic challenge" *Parameters* 1996–97 (Winter):81–91.

[24] M. G. Devost, "National security in the information age," Thesis, University of Vermont, 1995, available from the Terrorism Research Center.

Major Regional Powers

Major regional powers are more likely to conduct tactical IW strikes (i.e., against a small, specific set of targets to achieve a specific military goal) than launch an SIW attack. Part of the reason for this, as stated above, would be the potential consequences that a successful attack would have on the global economy. Although the United States may attempt to use the threat of nuclear retaliation as a more powerful punitive deterrent, it would be wise to focus on this reluctance and emphasize prevention (that is, removing any incentives for attacking) rather than punishment. This could be done through high-level discussions about information warfare to accentuate the interdependent nature of the world economy. The United States has a number of existing mechanisms for dialogues with Russia and the People's Republic of China on other issues (such as nuclear and biological weapons) and this issue could be pursued through the defense, diplomatic, or academic communities, or some combination.

Minor Regional Powers

Minor powers are less likely to have the resources to invest in a robust IW program, especially in the cyber reconnaissance to conduct a crippling SIW attack. They may, therefore, still doubt IW's potential. With the success of an SIW attack in question, a minor regional power might not risk escalation of the conflict by attempting such an attack. The United States can reinforce this inclination by emphasizing its ability to punish the attacker. To ensure that it will be in a position to retaliate (and therefore pose a credible threat), the United States should harden its military information infrastructure to the extent possible, and be able to operate at a basic level without the use of the civilian infrastructure. Even so, minor powers may still be willing to launch an attack out of desperation, if their state is on the verge of collapse under any circumstance. At that point, the United States is unlikely to be able to deter the threat at all, and would have to tailor its military operations to preempting such an attack, if possible. Ironically, this may include targeting the adversary's infrastructures, such as telecommunications or electric power.

Rogue States

Rogue states would have similar difficulties in conducting the necessary reconnaissance for an SIW attack, but the threat of punishment may be less effective, especially as the rulers appear to have minimum regard for their populations. Similarly, the United States is unlikely to influence a rogue state though discussions or limit it through treaties or agreements. Rogue states are less predictable than other states, in part because the United States lacks certain key elements of intelligence about such closed societies. Although any reliance on robust computer security would be dangerous, it is feasible for the United States to focus on a few systems of nation-wide importance and work with private industry to strengthen those. This would create a minimum threshold of security that may be expected to deny a minimum-level SIW attack, most likely consisting of openly available viruses and denial-of-service attack tools.

Terrorist Groups

Until terrorist groups display either the intent or ability to engage in IW attacks, they can be considered a low threat. Even so, they pose a significant problem for any deterrence policy because of the uncertainty as to whether their actions can even be deterred. Although terrorists are certainly determined adversaries, several characteristics of terrorist groups may indicate that certain activities can be deterred. First, they tend to attack soft rather than hardened targets. As with rogue states, a minimum threshold of security in U.S. infrastructures may be enough to influence a terrorist group to seek other targets. Second, the ability to punish the perpetrators may be a useful deterrent. Although some terrorists (especially suicide bombers) have no concern for punishment, those who plan and support the attack may. The current counterterrorism campaign is clearly an opportunity to establish the U.S. ability and commitment to pursue, locate, and eliminate the leadership of terrorist groups around the world. It should be executed, therefore, with the knowledge that it will likely establish the U.S. deterrent for such groups in the foreseeable future.

Conclusions

The U.S. information infrastructure was built for efficiency and convenience, and has become integrated into every aspect of the daily lives of the American people. Protecting this infrastructure is therefore a matter of national security. Deterrence can be a highly effective means of defending the infrastructure. Even so, it represents a significant challenge for U.S. policymakers. Although IW in many ways undermines specific aspects or counters certain deterrent tools, the United States should still be able to deter potential adversaries from SIW attacks, if they are approached with strategies tailored to their particular motivations and capabilities. This will not be simple, but it should be a high priority, especially for nations with a high capability (major regional states) or a high probability (rogue states) for SIW attacks. In many ways, the U.S. government can protect the nation through words—whether they threaten a specific group, open a dialogue with an individual country, or convince private industry to become more secure. But they have to be the right words, delivered at the right time.

Table 2: Strategies Most Likely to Deter SIW Attacks

Adversary	Form	Tool	Component of Need
Major power	Removing incentives	High-level policy discussions and exchanges	Communication
Minor power	Punishment	Emphasis of escalation	Credibility
Rogue state	Denial	Improved security of select civilian infrastructures	Intelligence
Terrorist group	Denial and punishment	Improved security of select civilian infrastructures Emphasis of willingness and ability to pursue and punish	Applicability